Verify text when signing

When the user signs an action/object make sure that the user is not able to edit the text that pop ups in the BankdID signing view. If the user can edit that one user could edit it and more easily trick another user into signing something.

Log in as one user and sign as another

Check that you can't log in as one user and then sign the result as another user. If this is in fact an issue depends on the application, how it is suppose to work.

DOS by queued upp auth requests

It is always possible to perform a DOS against a user, simply sending new authentication requests to that user. That is not a vulnerability, it is just how BankID works. But there exists a scenario where youi perform multiple authentication-requests, and these are then queued up, so when the user dismissed a auth request the enxt one in the queued pops up. If multiple requests are made, the previous ones should be invalidated.

Session fixation

Session fixation might be possible even with BankID. Sometimes you get a cookie when you enter a page, and when you have then authenticated the same cookie is used to retrieve a new cookie.

Test with user that has not been provided by customer

If you are provided with a number of users that are meant to have access to the page, test what happens if you authenticate with another user. This might be normal usage, that anyone can log in, and if that is the case then there is nothing to test. But if only limited number of users should be able to autehnticate, test with another user. If it is test-bankdID just generated a new bankid for random user.

Check if object can be changed after signing

If you sign objects of some kind, check that you can't change the object aftr the signature.